

TABLE OF CONTENTS

	Page
PRELIMINARY STATEMENT	1
STATEMENT OF FACTS	3
A. BDA Agreed to Use SWIFT Messages in Its Correspondent Banking Agreement With Wells Fargo.....	3
B. Wells Fargo Received Authenticated SWIFT Payment Orders From BDA	6
ARGUMENT	7
I. BDA Concedes Wells Fargo Acted in Accordance With the Agreed-Upon Security Procedure and Fails to Allege a Violation of the N.Y. U.C.C.....	8
A. BDA Admits That the Unauthorized Transfers Were “Effective” As Its Orders	9
1. Wells Fargo Complied with the Agreed-Upon Security Procedure	10
2. The Complaint Does Not Allege Bad Faith.....	12
B. The Unauthorized Transfers Were Sent By Individuals Who Accessed BDA’s Computer System Through Sources Controlled By BDA	15
C. “Know Your Customer” and Anti-Money Laundering Policies Are Irrelevant to BDA’s Statutory Claim and the Agreement’s Security Procedure	17
II. BDA’s Negligence and Breach of Contract Claims Are Precluded By Article 4-A of the N.Y. U.C.C.....	18
III. BDA Has Failed to State a Claim for Negligence in Any Event.....	22
A. The Agreement Prohibits Any Claim for Negligence.....	22
B. Wells Fargo Did Not Owe BDA a Duty of Care Independent of the Agreement.....	24
C. Wells Fargo Had No Duty to Prevent the Unauthorized Access of BDA’s Internal Systems	25
IV. Wells Fargo Did Not Breach the Agreement.....	26
CONCLUSION.....	29

TABLE OF AUTHORITIES

CASES	Page(s)
<i>2006 Frank Calandra, Jr. Irrevocable Tr. v. Signature Bank Corp.</i> , 816 F. Supp. 2d 222 (S.D.N.Y. 2011), <i>aff'd</i> 503 F. App'x 51 (2d Cir. 2012).....	19, 20
<i>Aleo Int'l, Ltd. v. Citibank, N.A.</i> , 612 N.Y.S.2d 540 (N.Y. Sup. Ct. N.Y. Cty. 1994).....	19
<i>Alitalia Linee Aeree Italiane, S.P.A. v. Airline Tariff Publ'g Co.</i> , 580 F. Supp. 2d 285 (S.D.N.Y. 2008).....	23
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662, 129 S. Ct. 1937 (2009).....	7, 8
<i>Banque Worms v. BankAmerica Int'l</i> , 568 N.Y.S.2d 541 (N.Y. 1991)	10, 15, 18
<i>Bell Alt. Corp. v. Twombly</i> , 550 U.S. 544, 127 S. Ct. 1955 (2007).....	8
<i>Braga Filho v. Interaudi Bank</i> , No. 03-cv-4795, 2008 WL 1752693 (S.D.N.Y. Apr. 16, 2008)	10
<i>Brower v. Nydic, Inc.</i> , 1 F. Supp. 2d 325 (S.D.N.Y. 1998)	28
<i>Calisch Assocs. Inc. v. Mfrs. Hanover Tr. Co.</i> , 542 N.Y.S.2d 644 (N.Y. App. Div. 1st Dep't 1989)	25
<i>Centre-Point Merch. Bank Ltd. v. Am. Express Bank Ltd.</i> , 913 F. Supp. 202 (S.D.N.Y. 1996)	21, 24
<i>Centre-Point Merch. Bank Ltd v. Am. Express Bank Ltd.</i> , No. 95-cv-5000, 2000 WL 1772874 (S.D.N.Y. Nov. 30, 2000).....	12, 26
<i>Clark-Fitzpatrick, Inc. v. Long Island R.R. Co.</i> , 521 N.Y.S.2d 653 (N.Y. 1987)	24
<i>Colnaghi, U.S.A., Ltd. v. Jewelers Protection Servs., Ltd.</i> , 595 N.Y.S.2d 381 (N.Y. 1993)	2, 22, 23

<i>Elite Investigations v. Bank of N.Y.</i> , No. 129790/2002, 2006 WL 3232185 (N.Y. Sup. Ct. N.Y. Cty. Sept. 8, 2006)	2, 12, 24, 25, 29
<i>First Inv'rs Corp. v. Liberty Mut. Ins. Co.</i> , 152 F.3d 162 (2d Cir. 1998).....	27
<i>Fischer & Mandell, LLP v. Citibank, N.A.</i> , 632 F.3d 793 (2d Cir. 2011).....	19, 21, 22
<i>Getty Petroleum Corp. v. Am. Express Travel Related Servs. Co., Inc.</i> , 660 N.Y.S.2d 689 (N.Y. 1997)	26
<i>Golden Door V&I, Inc. v. TD Bank</i> , 999 N.Y.S.2d 510 (N.Y. App. Div. 2d Dep't 2014)	19, 22
<i>Grain Traders, Inc. v. Citibank, N.A.</i> , 960 F. Supp. 784 (S.D.N.Y. 1997)	2, 7, 15
<i>Grain Traders, Inc. v. Citibank, N.A.</i> , 160 F.3d 97 (2d Cir. 1998).....	19
<i>Hidden Brook Air, Inc. v. Thabet Aviation Int'l Inc.</i> , 241 F. Supp. 2d 246 (S.D.N.Y. 2002).....	13
<i>I. Cruise.com Corp. v. Aliksanyan</i> , 847 N.Y.S.2d 896 (N.Y. Sup. Ct. N.Y. Cty. 2007).....	19
<i>In re Merrill Lynch & Co., Inc. Research Reports Sec. Litig.</i> , 273 F. Supp. 2d 351 (S.D.N.Y. 2003).....	3
<i>J. Walter Thompson, U.S.A., Inc. v. First BankAmericano</i> , 518 F.3d 128 (2d Cir. 2008).....	13, 14
<i>Kraus v. Visa Int'l Serv. Ass'n</i> , 756 N.Y.S.2d 853 (N.Y. App. Div. 1st Dep't 2003)	27
<i>Lerner v. Fleet Bank, N.A.</i> , 459 F.3d 273 (2d Cir. 2006).....	24
<i>Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.</i> , 597 F.3d 84 (2d Cir. 2010).....	2, 20
<i>Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Chemical Bank</i> , 456 N.Y.S.2d 742 (N.Y. 1982)	24
<i>Nigerian Nat'l Petroleum Corp. v. Citibank, N.A.</i> , No. 98-cv-4960, 1999 WL 558141 (S.D.N.Y. July 30, 1999).....	13

<i>Plaintiffs' State & Secs. Law Settlement Class Counsel v. Bank of N.Y. Mellon</i> , 985 N.Y.S.2d 398 (N.Y. Sup. Ct. N.Y. Cty. 2014).....	22, 24
<i>ReAmerica, S.A. v. Wells Fargo Bank Int'l</i> , 577 F.3d 102 (2d Cir. 2009).....	19
<i>Rothman v. Gregor</i> , 220 F.3d 81 (2d Cir. 2000).....	3
<i>SAA-A, Inc. v. Morgan Stanley Dean Witter & Co.</i> , 721 N.Y.S.2d 640 (N.Y. App. Div. 1st Dep't 2001)	28
<i>Silverman Partners, L.P. v. First Bank</i> , 687 F. Supp. 2d 269 (E.D.N.Y. 2010)	3, 25, 26
<i>Xi Mei Jai v. Intelli-Tec Sec. Servs., Inc.</i> , 981 N.Y.S.2d 79 (N.Y. App. Div. 1st Dep't 2014)	3, 28

STATUTES AND RULES

FED R. CIV. P. 12(b)(6)	1, 3, 7
N.Y. GEN. OBLIG. § 15-301(1).....	28
N.Y. U.C.C. § 1-304	13
N.Y. U.C.C. Art. 4-A, Prefatory Note	6
N.Y. U.C.C. § 4-A-102	18
N.Y. U.C.C. § 4-A-102 cmt.	19
N.Y. U.C.C. § 4-A-103(1)(d).....	9
N.Y. U.C.C. § 4-A-103(1)(e).....	9
N.Y. U.C.C. § 4-A-104 cmt. 6.....	10
N.Y. U.C.C. § 4-A-105(1)(c).....	9
N.Y. U.C.C. § 4-A-105(1)(f)	13
N.Y. U.C.C. § 4-A-105 cmt. 2	14
N.Y. U.C.C. § 4-A-202(1)	21
N.Y. U.C.C. § 4-A-202(2)	2, 9, 16, 21
N.Y. U.C.C. § 4-A-202(6)	13, 21

N.Y. U.C.C. § 4-A-203(1)(b).....	2, 15, 16
N.Y. U.C.C. § 4-A-203(2)	16
N.Y. U.C.C. § 4-A-203 cmt. 5	10, 15, 17
N.Y. U.C.C. § 4-A-204(1)	8, 9, 15
N.Y. U.C.C. § 4-A-204 cmt. 1	16

Defendant Wells Fargo Bank, N.A. (“Wells Fargo”) respectfully moves to dismiss the Complaint with prejudice pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.

PRELIMINARY STATEMENT

In this case, Banco del Austro, S.A. (“Plaintiff” or “BDA”),¹ an Ecuadorian bank, seeks to recover funds from Wells Fargo that it has been unable to recover from sophisticated computer hackers. These hackers (i) obtained unique computer access information and credentials from one of BDA’s employees; (ii) used these credentials to access BDA’s computer network; (iii) sent otherwise validly authorized wire transfer payment orders to Wells Fargo over a secure network; and (iv) absconded with the resulting funds after they were transferred by Wells Fargo.

While BDA is pursuing the persons who hacked its system, this lawsuit is an attempt to hold Wells Fargo liable for doing nothing more than *exactly* what it agreed to do when it became BDA’s correspondent bank – execute authenticated and authorized payment orders that originated from BDA’s computers. Indeed, BDA acknowledges that the payment orders at issue that Wells Fargo received were *identical* to hundreds of payment orders and wire transfer instructions that BDA sent Wells Fargo over the course of their four-year relationship. BDA itself did not even determine that the payment orders at issue were unauthorized and that its own system had been compromised until over a week after the first fraudulent transfer request. Despite the fact that BDA’s loss resulted from its own failure to monitor its systems and to detect the fraudulent payment orders, BDA asks that the Court hold Wells Fargo responsible for BDA’s security shortfalls. In so doing BDA seeks to create duties that go well beyond those contained

¹ Unless otherwise noted, capitalized terms are as defined in Plaintiff’s Complaint, filed on January 7, 2016, and attached as Exhibit A to Wells Fargo’s Notice of Removal (ECF No. 1) and as Exhibit 1 to the Declaration of Jeffery J. Chapman, submitted herewith (the “Complaint”). All references to “Ex. []” are to the exhibits to the Declaration of Jeffrey J. Chapman.

in any banking relationship, essentially arguing that Wells Fargo was obligated to detect and prevent these fraudulent payment orders.

Wells Fargo did not agree to assume responsibility for BDA's security, and is not liable for the breaches of that security which led to the fraudulent payment orders at issue. BDA alleges that Wells Fargo failed to comply with the New York Uniform Commercial Code (the "N.Y. U.C.C." or "Uniform Commercial Code"), breached the terms of the agreement governing their banking relationship, and violated an unspecified duty of care. Each of these claims suffer from fatal flaws.

First, BDA admits that the payment orders at issue were sent from its own computer system and were authenticated pursuant to its agreement with Wells Fargo, making them "effective as its order" under Section 4-A-202(2) of the N.Y. U.C.C. and exempting Wells Fargo from any liability for its loss. *See Grain Traders, Inc. v. Citibank, N.A.*, 960 F. Supp. 784, 786, 792 (S.D.N.Y. 1997); *Elite Investigations v. Bank of N.Y.*, No. 129790/2002, 2006 WL 3232185, at *4-5 (N.Y. Sup. Ct. N.Y. Cty. Sept. 8, 2006). Nor can BDA meet its affirmative burden under Section 4-A-203(1)(b) of the Uniform Commercial Code of proving that the hackers did not obtain access to its system by stealing information under its control. Indeed, BDA admits that its own systems were hacked. Further, the conduct at issue – Wells Fargo's processing of electronic funds transfer orders – is governed *exclusively* by the N.Y. U.C.C., precluding BDA's common law negligence and breach of contract claims. *See Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 597 F.3d 84, 89-90 (2d Cir. 2010). Even if BDA's negligence claim were not precluded, it is barred by the terms of BDA's agreement with Wells Fargo (which precludes claims for simple negligence) and the legal principle that Wells Fargo did not owe BDA a duty of care based on the federal law referenced in the parties' agreement upon which BDA relies. *See Colnaghi*,

U.S.A., Ltd. v. Jewelers Protection Servs., Ltd., 595 N.Y.S.2d 381, 381 (N.Y. 1993); *see also Silverman Partners, L.P. v. First Bank*, 687 F. Supp. 2d 269, 282 (E.D.N.Y. 2010). Finally, BDA's breach of contract claim fails both because BDA admits that Wells Fargo complied with the only terms of the contract at issue and because BDA is prohibited from incorporating its extra-contractual "duties" into the parties' agreement. *See Xi Mei Jai v. Intelli-Tec Sec. Servs., Inc.*, 981 N.Y.S.2d 79, 80-81 (N.Y. App. Div. 1st Dep't 2014).

STATEMENT OF FACTS²

A. BDA Agreed to Use SWIFT Messages in Its Correspondent Banking Agreement With Wells Fargo.

In February of 2011, BDA and Wells Fargo entered into a correspondent banking relationship (the "Relationship") that allowed BDA to "conduct international banking operations, including funding overseas payments and wiring transfers requested by its clients in Ecuador" through its account with Wells Fargo (the "Account"). *See* Compl. ¶¶ 8-9. The Relationship was governed by Wells Fargo's Terms and Conditions for Global Financial Institutions (the "Agreement"), which BDA understood and acknowledged upon entering into the Relationship. *See* Compl. Ex. A (letter signed by BDA acknowledging receipt of the Agreement). Under the terms of the Agreement, BDA utilized its connection to the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") network, a widely used system that allows banks and other financial institutions to send secure messages and instructions that are authenticated and contain each institution's unique Business Identifier Code ("BIC"). *See* Ex. 2 at 14. SWIFT messages, like the payment orders at issue in this case, are among the most widely used and

² In examining a motion to dismiss pursuant to Rule 12(b)(6), the Court may consider documents referenced in or attached to a complaint, documents "integral" to the complaint, even if not specifically attached or incorporated by reference, and items subject to judicial notice, such as public records and Plaintiff's filings in other actions. *See, e.g., Rothman v. Gregor*, 220 F.3d 81, 92 (2d Cir. 2000); *In re Merrill Lynch & Co., Inc. Research Reports Sec. Litig.*, 273 F. Supp. 2d 351, 356-57 (S.D.N.Y. 2003).

secure means of initiating wire transfer requests and payment orders. Before banks begin transferring funds pursuant to messages sent on the SWIFT network, they undergo a detailed authentication process to ensure that any payment order that is sent does in fact emanate from, and is duly authorized by, the sending entity. *See* Ex. 2 at 11 (defining authentication as the “process that SWIFT uses to confirm the identity of the sender or receiver of a message, or to prove the integrity of specific information. Message authentication determines the source of a message, and verifies that no-one has modified or replaced the message during transit.”). Pursuant to its contract with Wells Fargo, BDA agreed to use the SWIFT network, which “must be accessed from within BDA’s computer system,” to generate wire transfer payment orders, to communicate with Wells Fargo, and to send instructions regarding its correspondent banking Account. Compl. ¶ 18. The terms and conditions to which BDA agreed contained a variety of provisions regarding the authenticity of its instructions to Wells Fargo, including the payment orders at issue. For example:

- “[BDA] must utilize authenticated SWIFT message formats . . . and Wells Fargo *will be entitled to rely upon all such messages appearing to have been sent by [BDA].*” Compl. Ex. A ¶ 2.1 (emphasis added).
- “All payment orders . . . must be transmitted to Wells Fargo in compliance with Security Procedures. Wells Fargo will verify the authenticity of payment orders pursuant to the Security Procedures. Any payment order authenticated under the Security Procedures will be the authorized order of [BDA], if Wells Fargo accepts the order in good faith.” *Id.* ¶ 3.1
- “The following Security Procedures will be used to verify that [BDA] is the originator of a payment order For SWIFT, the SWIFT Authentication procedures in accordance with the SWIFT User Handbook [BDA] agrees that the above described Security Procedures are commercially reasonable” *Id.*; Compl. ¶ 19.
- “Upon receipt of a payment order from [BDA] authenticated in accordance with Security Procedures contained herein Wells Fargo is authorized to debit [BDA’s] Account . . . and transfer or pay funds upon the value date.” Compl. Ex. A ¶ 3.4.

The Agreement also contained language about Wells Fargo’s compliance with the laws of

the United States and the State of New York. *See id.* ¶ 7.7 (stating that the Agreement would be “governed by and construed in accordance with the Laws of the US and the State of New York, including (without limitation) Articles 3, 4, 4A, and 5 of the Uniform Commercial Code” and by “applicable rules of . . . the Board of Governors of the Federal Reserve System of the US, the rules of clearing houses and similar associations . . . and general US commercial bank practices applicable in connection with [BDA’s Account]”). Specifically, Wells Fargo informed BDA that it “intend[ed] to comply with all laws of the US . . . including without limitation the USA PATRIOT Act” and “regulations of the United States Department of the Treasury and Office of Foreign Assets Control” (“OFAC”). *Id.* ¶ 7.8. Compliance with such laws was designed to “help the US government fight the funding of terrorism and money laundering activities.” *Id.* BDA acknowledged that Wells Fargo’s compliance with such laws “may affect the transactions [BDA] may conduct with, or through, Wells Fargo” and that its Account could be “subject to attachment, levy, seizure, and garnishment.” *Id.* ¶¶ 7.7-7.8; Compl. ¶¶ 12-13. The Agreement does not contain a representation that Wells Fargo would monitor transactions in an effort to detect suspicious activity that might be occurring as a result of breaches of its customers’ own security.

Finally, BDA agreed that any liability imposed upon Wells Fargo will be limited to “actual damages that are the direct result of Wells Fargo’s gross negligence or willful misconduct, which will be determined in accordance with the commercial standards of Wells Fargo’s peers in the US banking industry and applicable Laws.” Compl. Ex. A ¶ 7.15. The Agreement also made clear that it constituted the “entire agreement and understanding” between Wells Fargo and BDA and that it “may not be changed orally.” *Id.* ¶ 7.19.

B. Wells Fargo Received Authenticated SWIFT Payment Orders From BDA.

On January 12, 2015, Wells Fargo began receiving the SWIFT payment orders at issue, which BDA admits “originat[ed] from BDA’s SWIFT terminal,” were authenticated by SWIFT, and which Wells Fargo processed in accordance with the terms of the Agreement. Compl. ¶¶ 20, 22-23, 31; Compl. Ex. B. These SWIFT payment orders, which BDA attaches to the Complaint, contained BDA’s unique SWIFT BIC identification code, confirming that they were authenticated pursuant to the Agreement and that they were indistinguishable from any other SWIFT payment order Wells Fargo received from BDA during their Relationship. *Compare* Compl. Ex. B (indicating that the payment orders were sent from the SWIFT terminal of “AUSTECEQX100” or “AUSTECEQXXXX”) *with* Ex. 3 (confirming that “AUSTECEQX” is the unique SWIFT BIC identification code for BDA). More than one week after the first of these payment orders was sent by BDA, BDA “discovered that . . . an unauthorized user [had] remotely accessed BDA’s computer system after hours, logged into the SWIFT network purporting to be BDA, and redirected transactions to new beneficiaries” Compl. ¶ 31.

On January 21, 2015, BDA alleges that it notified Wells Fargo that the payment orders at issue were actually the result of criminals hacking into its computer system, and attempted to cancel the transactions. *Id.* ¶¶ 22-23, 31-32. Upon receiving notice of the fraudulent nature of the Unauthorized Transfers, Wells Fargo attempted to recall and recover the funds that were sent from BDA’s Account as a result of the fraud. However, due to the amount of time that had elapsed since the first Unauthorized Transfer and when Wells Fargo received the fraud notification, the payment orders had been fully processed.³ *See* Compl. Ex. A ¶ 3.6 (noting that

³ Indeed, as the Prefatory Note to Article 4-A explains, “[h]igh speed” is a “predominant characteristic” of electronic funds transfers, and “[m]ost funds transfers are completed on the same day, even in complex transactions in which there are several intermediary banks in the

Wells Fargo's attempts to cancel an executed payment order "may require the consent of third parties" and that Wells Fargo will not be liable for the failure of an attempted cancellation). Wells Fargo was able to make a partial refund to BDA, but was unable to recall the balance of the fraudulently transferred funds from the beneficiary banks that received the funds. *Id.* ¶ 34. In April 2015, BDA initiated legal proceedings in Hong Kong – where nine of the twelve wire transfers were sent – in order to recover the funds directly from the beneficiaries (the "Hong Kong Proceeding"). *Id.* ¶¶ 23, 36. In the Hong Kong Proceeding, BDA explained that the unauthorized transfers were made by "an unidentified unauthorised computer user [who] accessed [BDA's] computer system remotely using the unique log-in information and credentials belonging to one of [its] employees." Ex. 4 at 2. BDA further stated that the unauthorized user "logged on to the SWIFT Network and purported to authorized the transactions as [BDA]" and "fraudulently caused funds to be transferred, without authorization, to various accounts . . . by way of re-issuing previously cancelled or rejected transactions that remained in the SWIFT outbox but altered the amounts, the beneficiary, and the destination" *Id.* at 2-3.

Apparently unable to recover from those who perpetrated the theft, BDA filed suit against Wells Fargo on January 7, 2016 in New York Supreme Court alleging a violation of the N.Y. U.C.C. and common law breach of contract and negligence claims. Wells Fargo removed this action on January 28, 2016, and now moves to dismiss BDA's Complaint with prejudice.

ARGUMENT

A complaint must be dismissed under Federal Rule of Civil Procedure 12(b)(6) if it does not "contain sufficient factual matter, accepted as true, 'to state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 1949 (2009) (quoting *Bell*

transmission chain." N.Y. U.C.C. Art. 4-A, Prefatory Note; *see also Grain Traders*, 960 F. Supp. at 786-87.

Alt. Corp. v. Twombly, 550 U.S. 544, 570, 127 S. Ct. 1955, 1974 (2007)). Well-pleaded factual allegations are accepted, but in order to state grounds for valid relief, a complaint cannot rely on conclusory statements and legal conclusions, which are not “entitled to the assumption of truth.” *Id.* at 679; 129 S. Ct. at 1950. A complaint further is insufficient to state a claim where it is supported only by “naked assertions devoid of further factual enhancement” that fail to establish that a defendant is liable for the alleged conduct. *Id.* at 678; 129 S. Ct. at 1949 (quoting *Twombly*, 550 U.S. at 557; 127 S. Ct. at 1966). Finally, any factual allegations cited as the basis for a plaintiff’s claim “must be enough to raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555; 127 S. Ct. at 1965.

I. BDA Concedes Wells Fargo Acted in Accordance With the Agreed-Upon Security Procedure and Fails to Allege a Violation of the N.Y. U.C.C.

As BDA admits in the Complaint, and as it agreed when entering into the Relationship with Wells Fargo, the mechanics and execution of wire transfers and payment order requests made pursuant to the Agreement are governed by the New York Uniform Commercial Code. Compl. ¶¶ 64-65; Compl. Ex. A ¶¶ 3.1, 7.7. BDA alleges that Wells Fargo violated Section 4-A-204(1) of the Uniform Commercial Code by failing to refund the balance of the Unauthorized Transfers that was not returned to BDA. Compl. ¶¶ 47-48, 64-65. BDA further alleges that Wells Fargo is liable because it did not “accept the Unauthorized Transfers in good faith and in compliance with the security procedure agreed-upon in the Agreement.” *Id.* ¶ 51. However, the Complaint contains no allegation that Wells Fargo failed to verify the authenticity of the SWIFT payment orders, which BDA admits were sent from its own computer system and were indistinguishable from otherwise valid payment orders. *Id.* ¶¶ 18, 20, 31. These admissions are fatal to BDA’s claims.

A. BDA Admits That the Unauthorized Transfers Were “Effective” As Its Orders.

Section 4-A-204(1), upon which BDA bases its statutory claim against Wells Fargo, states that when a receiving bank such as Wells Fargo,⁴ “accepts a payment order issued in the name of its customer as sender [BDA] which is (a) *not authorized* and *not effective* as the order of the customer under Section 4-A-202, or (b) not enforceable, in whole or in part, against the customer under Section 4-A-203” then the receiving bank shall refund the payment.⁵ N.Y. U.C.C. § 4-A-204(1) (emphasis added). It is clear from the pleadings in this case that the payment orders were “effective” as BDA’s orders and that as a result Wells Fargo has no obligation to refund the transfers under the N.Y. U.C.C.

Section 4-A-202(2) of the Uniform Commercial Code states:

If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, *whether or not authorized*, if (a) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (b) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

N.Y. U.C.C. § 4-A-202(2) (emphasis added). As contemplated by this Section, BDA and Wells Fargo agreed that the authenticity of BDA’s payment orders would be verified by SWIFT and that this security procedure was a commercially reasonable method of authentication. *See* Compl. Ex. A ¶ 3.1 (“[BDA] agrees that the above described Security Procedures [including

⁴ A receiving bank is defined as “the bank to which the sender’s instruction is addressed.” N.Y. U.C.C. § 4-A-103(1)(d).

⁵ In this case, BDA is both the customer and sender under the N.Y. U.C.C. *See* N.Y. U.C.C. § 4-A-103(1)(e) (“‘Sender’ means the person giving the instruction to the receiving bank.”); *id.* § 4-A-105(1)(c) (“‘Customer’ means a person, including a bank, having an account with a bank or from whom a bank has agreed to receive payment orders.”).

SWIFT authentication] are commercially reasonable”); *see also* N.Y. U.C.C. § 4-A-104 cmt. 6 (referencing SWIFT as a funds transfer system contemplated by Article 4-A). The only outstanding questions for the Court are therefore whether the Complaint contains any well-pled factual allegations that Wells Fargo did not accept the payment orders in compliance with the security procedure and pursuant to the terms of the Agreement or that Wells Fargo acted in bad faith. *See Braga Filho v. Interaudi Bank*, No. 03-cv-4795, 2008 WL 1752693, at *3 (S.D.N.Y. Apr. 16, 2008) (“Section 4-A-202(2) provides that when a customer has agreed to a bank’s security procedure, the customer will bear the risk of loss if the security procedure was ‘commercially reasonable’ and if the bank followed that procedure.”); *Banque Worms v. BankAmerica Int’l*, 568 N.Y.S.2d 541, 549 (N.Y. 1991) (“[U]nder N.Y. U.C.C. 4-A-202(2), if a bank accepts a payment order that purports to be that of its customer after verifying its authenticity through an agreed upon security procedure, the customer is bound to pay the order *even if* the payment order was not authorized.”) (emphasis added); *see also* N.Y. U.C.C. § 4-A-203 cmt. 5 (“The effect of Section 4-A-202(2) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure.”).

1. Wells Fargo Complied with the Agreed-Upon Security Procedure.

Even reading the Complaint in its most favorable light, there is no question that Wells Fargo acted pursuant to properly authenticated SWIFT messages from BDA. BDA *admits* that Wells Fargo accepted the SWIFT messages at issue in accordance with the commercially reasonable security procedure detailed in Paragraph 3.1 of the Agreement, therefore fulfilling Wells Fargo’s obligations under Section 4-A-202 of the N.Y. U.C.C. The Agreement states that for communications sent via the SWIFT network, the security procedure “used to verify that

[BDA] is the originator of a payment order, or is the sender of other communication requesting an amendment, cancellation or other action regarding a payment order” is “SWIFT Authentication.” Compl. Ex. A ¶ 3.1; *see also* Compl. ¶ 19. The pleadings in this case make clear that the payment orders that led to the Unauthorized Transfers were authenticated by SWIFT, were sent from BDA’s SWIFT terminal using BDA’s SWIFT network access, contained BDA’s unique BIC identification code, and were facially identical to otherwise validly authorized payment orders originating from BDA. *See* Compl. ¶¶ 18-20, 31 (admitting that the parties agreed that SWIFT authentication would be used as the security procedure under the Agreement and that the payment orders at issue originated from BDA and were indistinguishable from those authorized by BDA); Compl. Ex. B; Ex. 3; *see also* Ex. 4 at 2-3 (stating in the Hong Kong Proceeding that the SWIFT payment orders were sent by a user who “logged on to the SWIFT Network and purported to authorize the transactions as [BDA]” by “re-issuing previously cancelled or rejected transactions that remained in [BDA’s] SWIFT outbox”). Nor is there a dispute that “Wells Fargo [was] entitled to rely upon” all “authenticated SWIFT message[s] . . . appearing to have been sent by [BDA].” Compl. Ex. A ¶ 2.1. As a result, Wells Fargo complied with the Agreement’s security procedures by verifying the authenticity of the payment orders, and the Court’s inquiry need not proceed further.

To impose liability upon Wells Fargo for *complying* with the security procedures contained in the Agreement would render Article 4-A meaningless. BDA cannot now undo the Agreement simply because, in hindsight, it might have sought different or additional security procedures. *See* Compl. ¶ 20 (noting that “[A]though the SWIFT Authentication procedure would be used to verify whether BDA was the originator of a payment order . . . it could not be used to verify whether suspicious activity originating from BDA’s SWIFT terminal was

fraudulent . . . or in fact authorized by BDA”). But the Agreement – and therefore the Uniform Commercial Code – obligated Wells Fargo only to verify that the SWIFT payment orders received from BDA were authenticated, not to patrol BDA’s computer network to guard against the third-party hacking that rendered the Unauthorized Transfers indistinguishable from other payment orders. *Id.* ¶¶ 19-20.

By verifying that BDA appeared to be the originator of the payment orders at issue, Wells Fargo ensured that they were “effective as the order” of BDA, and BDA’s statutory claim must therefore be dismissed. *See Centre-Point Merch. Bank Ltd v. Am. Express Bank Ltd.*, No. 95-cv-5000, 2000 WL 1772874, at *5-6 (S.D.N.Y. Nov. 30, 2000) (dismissing Article 4-A claim because defendant complied with the agreed-upon security procedure, while noting both that plaintiff was in a position to discover the fraud at issue much earlier than it did and that simply because defendant “did not recognize the fraudulent work of [plaintiff’s] employee . . . does not indicate a failure to comply with the security procedure”); *Elite Investigations*, 2006 WL 3232185, at *4 (“Under [N.Y. U.C.C. § 4-A-202(2)], if the bank adheres to commercially reasonable security measures to which the customer agreed and the customer has not instructed the bank to deny electronic fund payment orders, then the receiving bank’s acceptance of the payment order is an effective customer order.”).

2. The Complaint Does Not Allege Bad Faith.

Because Wells Fargo complied with the Agreement’s security procedure, it acted in good faith under the N.Y. U.C.C. BDA attempts to allege that Wells Fargo did not act in good faith because it “failed to detect, block and report the Unauthorized Transfers” and “failed to observe reasonable commercial standards of fair dealing.” Compl. ¶¶ 59, 61-63. These conclusory claims are not based upon the terms of the Agreement, the Uniform Commercial Code, or any

case law. Rather, they are based solely on alleged representations made by Wells Fargo and invented common law duties. Not only do such claims fail as a matter of law, *see infra* Sections III and IV, but they are irrelevant to an analysis of Wells Fargo's compliance with Section 4-A-202. *See* N.Y. U.C.C. § 4-A-202(6) (stating that the "rights and obligations arising under" Section 4-A-202 "may not be varied by agreement").

Article 4-A of the Uniform Commercial Code defines good faith as "honesty in fact and the observance of reasonable commercial standards of fair dealing." N.Y. U.C.C. § 4-A-105(1)(f). In examining this definition of good faith, the Second Circuit has noted that the "requirement incorporates standards of honesty and fair dealing but not of negligence. In other words, the good faith requirement does not impose a standard of care but, rather, a standard of *fair dealing*." *J. Walter Thompson, U.S.A., Inc. v. First BankAmericano*, 518 F.3d 128, 139 (2d Cir. 2008) (emphasis in original). The Court then dismissed the statutory claim at issue, finding that there were no allegations that the bank "acted unfairly or dishonestly" and that while allegations that the bank should have "employed more advanced fraud detection capabilities" might "arguably establish negligence, they do not demonstrate a lack of honesty in fact or a failure to observe reasonable commercial standards of fair dealing." *Id.* at 139-40 (quotations omitted). New York courts examining the Uniform Commercial Code's general imposition of an obligation of good faith, *see* N.Y. U.C.C. § 1-304, have similarly held that a plaintiff seeking to demonstrate that a defendant failed to act in good faith must show that it "acted dishonestly." *Hidden Brook Air, Inc. v. Thabet Aviation Int'l Inc.*, 241 F. Supp. 2d 246, 275 (S.D.N.Y. 2002); *cf. Nigerian Nat'l Petroleum Corp. v. Citibank, N.A.*, No. 98-cv-4960, 1999 WL 558141, at *6 (S.D.N.Y. July 30, 1999) (noting that under New York law, "a bank is liable for commercial bad faith only where it acts dishonestly – where it has actual knowledge of facts and circumstances

that amount to bad faith, thus itself becoming a participant in a fraudulent scheme”) (quotation omitted).

The Complaint contains no allegation that Wells Fargo acted in a dishonest manner or had knowledge of the underlying scheme perpetrated against BDA. BDA conclusively asserts that Wells Fargo should have somehow detected the Unauthorized Transfers due to their “unusual or anomalous characteristics.” Compl. ¶¶ 61-63. But these at most show a failure of diligence, not bad faith, and are thus insufficient as a matter of law. *See J. Walter Thompson*, 518 F.3d at 140. And in any event these “unusual or anomalous characteristics” do not even suggest failures of diligence. The alleged “unusual” events include authenticated SWIFT payment orders that were: (i) sent outside of normal operating hours; (ii) in unusual amounts; (iii) to unusual and repeat beneficiaries in unusual geographic locations; and (iv) in unusual frequencies. *Id.* ¶ 26. But there is nothing unusual about these characteristics beyond BDA’s own speculation. Indeed, the “[f]unds transfer business is frequently transacted by banks outside of general banking hours.” N.Y. U.C.C. § 4-A-105 cmt. 2. As alleged in the Complaint, BDA itself notified Wells Fargo of the Unauthorized Transfers at approximately 11:00 pm. *See* Compl. ¶ 28 (stating that BDA alerted Wells Fargo of an Unauthorized Transfer “three hours after” the SWIFT payment order was sent at 7:56 pm).

BDA is essentially requesting that the Court require banks to monitor incoming wire transfer payment orders to ensure that they are not in unusual amounts, at odds times of the day, and are not sent to “unusual geographic locations” such as the international banking centers of Hong Kong and the United Arab Emirates. Compl. ¶ 26. Doing so would not only impose a tremendous strain on every New York bank that processes wire transfers, but would also defeat the efficiencies gained by using electronic funds transfers and impose far greater transaction

costs on customers such as BDA. *See Grain Traders*, 960 F. Supp. at 786-87 (dismissing an Article 4-A claim and noting that banks processing funds transfers cannot be expected to conduct “due diligence” due to the “high speed and low cost” nature of the transactions); *Banque Worms*, 568 N.Y.S.2d at 545-46 (explaining that electronic funds transfers “have become the preferred method . . . to effect payments” because they are “faster” than traditional instruments and can be completed “at a relatively low cost”).

Conclusory allegations aside, there is nothing in the Complaint suggesting that Wells Fargo acted dishonestly by processing the payment orders after they were authenticated by SWIFT in accordance with the Agreement. Wells Fargo did exactly what it was asked to do – receive SWIFT payment orders from BDA, ensure that they were authenticated by SWIFT, and process them in accordance with the instructions. *See Grain Traders*, 960 F. Supp. at 786, 792 (dismissing an allegation that defendant bank violated the good faith requirement of Article 4-A because it “did all that it was required to do,” and arguments that it “knew or should have known” of potential issues with an otherwise valid payment order were “inconsistent with the concept of funds transfers as well as the letter and spirit of Article 4-A”).

B. The Unauthorized Transfers Were Sent By Individuals Who Accessed BDA’s Computer System Through Sources Controlled By BDA.

BDA cannot rely on the refund provision of Section 4-A-204(1) because it cannot meet its burden of proving under Section 4-A-203(1)(b) that “the person committing the fraud [the hackers] did not obtain the confidential information” that allowed them to access BDA’s SWIFT terminal and computer systems “from an agent or former agent of [BDA] or from a source

controlled by [BDA].”⁶ N.Y. U.C.C. § 4-A-203 cmt. 5. Specifically, Section 4-A-203(1)(b) states that once a receiving bank, such as Wells Fargo, demonstrates compliance with Section 4-A-202(2), the *only* way that it will be deemed liable for the loss of a customer, such as BDA, is if BDA can prove that the fraudulent order was not caused “directly or indirectly” (i) by a person entrusted to act for BDA or (ii) by someone who “obtained access to transmitting facilities of [BDA] or who obtained, from a source controlled by [BDA] and without authority of [Wells Fargo], information facilitating breach of the security procedure, regardless of how the information was obtained or whether [BDA] was at fault.” N.Y. U.C.C. § 4-A-203(1)(b) (also noting that “information” includes “any access device [and] computer software”); *see also id.* § 4-A-203(2) (confirming that Section 4-A-203 also applies to amendments to payment orders).

BDA does not – and cannot – assert the protections of Section 4-A-203 because it has admitted both in the Complaint and in the Hong Kong Proceeding that the Unauthorized Transfers were caused by an unauthorized user who accessed BDA’s computer systems after obtaining “the unique log-in information and credentials belonging to one of [BDA’s] employees.” Ex. 4 at 2; *see also* Compl. ¶ 31 (alleging that “for each Unauthorized Transfer, an

⁶ The official comment to Section 4-A-204 states:

§ 4A-204 applies *only* to cases in which (i) no commercially reasonable security procedure is in effect, (ii) the bank did not comply with a commercially reasonable security procedure that was in effect, (iii) the sender can prove, pursuant to Section 4A-203(1)(b), that the culprit did not obtain confidential security information controlled by the customer, or (iv) the bank, pursuant to § 4A-203(1)(a) agreed to take all or part of the loss resulting from an unauthorized payment order.

N.Y. U.C.C. § 4-A-204 cmt. 1 (emphasis added). None of these four circumstances apply to BDA’s claim. First, the Agreement confirms that BDA acknowledged that the security procedure of SWIFT authentication used to verify the payment orders at issue was commercially reasonable. Second, as explained above, Wells Fargo complied with the security procedure. *See supra* Section I.A.1. Third, as explained herein, BDA has admitted that the wrongdoer who caused the Unauthorized Transfers did so by obtaining BDA’s confidential security information. Finally, BDA has not alleged, nor does the Agreement support, a claim that Wells Fargo agreed to assume the loss from an unauthorized payment order.

unauthorized user . . . accessed BDA's computer system . . . logged onto the SWIFT network purporting to be BDA, and redirected transactions to new beneficiaries"). There is no allegation that the wrongdoer responsible for the Unauthorized Transfers was acting with the authority of Wells Fargo. Thus, BDA has admitted (i) that the payment orders at issue were caused indirectly by a person entrusted to act on its behalf – the employee whose computer log-in information and credentials were stolen – or, alternatively, (ii) that the hackers behind the Unauthorized Transfers used this information to access BDA's transmitting facilities (its SWIFT terminal) and breach the security procedure. *See* Ex. 4 at 2-3; Compl. ¶ 31. Based on these admissions, BDA is prohibited from shifting liability for its loss to Wells Fargo. *See* N.Y. U.C.C. § 4-A-203 cmt. 5 (noting that, if a bank complies with Section 4-A-202(2), a customer such as BDA can avoid a loss stemming from a fraudulent payment order "if the customer can prove that the fraud was not committed by a person described in [4-A-203(1)(b)]," which BDA cannot).

C. "Know Your Customer" and Anti-Money Laundering Policies Are Irrelevant to BDA's Statutory Claim and the Agreement's Security Procedure.

Finally, BDA misconstrues the security procedures contained in the Agreement by attempting to read into the procedure alleged duties that Wells Fargo owed BDA pursuant to "applicable laws and general US commercial bank practices," which include unspecified "fraud detection" and "know your customer" programs allegedly "trumpeted" by Wells Fargo. Compl. ¶¶ 53-62. However, as explained above, the Agreement's reference to governing law and "general US commercial bank practices" was instead simply providing that Wells Fargo would honor legal "attachment, levy, seizure, and garnishment" proceedings that might impact the Account and would complying with the Treasury Department's anti-money laundering regulations. Compl. Ex. A ¶¶ 7.7-7.8. There is no suggestion in the Agreement that Wells Fargo was undertaking any affirmative duties for the benefit of BDA beyond processing electronic

funds transfers in accordance with its terms. Any “know your customer” and “fraud detection policies and procedures designed to detect and deter suspicious activity” in the Account, Compl. ¶ 55, refer to Wells Fargo’s efforts to “help the US government fight the funding of terrorism and money laundering activities,” which might as a result require it to “obtain, verify, and record information that identifies each person who opens an account.” Compl. Ex. A ¶ 7.8. Wells Fargo’s compliance with such laws and regulations was simply not a part of the agreed-upon security procedure for verifying whether or not BDA was the originator of a payment order sent via SWIFT, and the Agreement was clear that the only such security procedure would be SWIFT authentication. *See id.* ¶ 3.1 (“The following Security Procedures will be used to verify that [BDA] is the originator of a payment order . . . [f]or SWIFT, the SWIFT Authentication procedures”); Compl. ¶ 52. Nowhere does the Agreement suggest that Wells Fargo agreed to the additional security procedure of monitoring each and every wire transfer request or payment order to ensure that it was not the result of a third-party hacking into its customer’s computer network. Compl. ¶¶ 18, 20, 31.

II. BDA’s Negligence and Breach of Contract Claims Are Precluded By Article 4-A of the N.Y. U.C.C.

Analysis of BDA’s claims need not proceed beyond the question of compliance with the Uniform Commercial Code, as any common law claims alleged by BDA, including those for negligence and breach of contract, are precluded by Article 4-A. The New York legislature enacted Article 4-A for the specific purpose of defining the exclusive rights and obligations of entities involved in the electronic funds transfers and payment orders at issue here. N.Y. U.C.C. § 4-A-102; *see also Banque Worms*, 568 N.Y.S.2d at 545-48 (discussing the history of Article 4-A and its goal of promoting “uniformity in the treatment of electronic funds transfers”). The Official Comment to Section 4-A-102 of the N.Y. U.C.C. states that the provisions of Article 4-

A “are intended to be the *exclusive* means of determining the rights, duties and liabilities of the affected parties in any situation” arising under Article 4-A, and that “resort to principals of law or equity outside of Article 4A is not appropriate to create rights, duties and liabilities inconsistent with those stated in this Article.” N.Y. U.C.C. § 4-A-102 cmt. (emphasis added).

The Second Circuit has determined that this language necessarily means that Article 4-A “preclude[s] common law claims when such claims would impose liability inconsistent with the rights and liabilities expressly created by Article 4-A.” *Grain Traders, Inc. v. Citibank, N.A.*, 160 F.3d 97, 103 (2d Cir. 1998); *see also ReAmerica, S.A. v. Wells Fargo Bank Int’l*, 577 F.3d 102, 106-07 (2d Cir. 2009) (common law statute of limitations did not apply to claim involving wire transfer, which was instead governed by the limitations period of the Uniform Commercial Code, “preclude[ing] [plaintiff’s] common law negligence claim”). As a result, “there is no claim for negligence unless the conduct complained of was not in conformity with Article 4-A.” *Fischer & Mandell, LLP v. Citibank, N.A.*, 632 F.3d 793, 801 (2d Cir. 2011) (quotation omitted); *see also Aleo Int’l, Ltd. v. Citibank, N.A.*, 612 N.Y.S.2d 540, 541 (N.Y. Sup. Ct. N.Y. Cty. 1994) (“Article 4-A does not include any provision for a cause of action in negligence.”). Breach of contract claims are similarly barred. *See 2006 Frank Calandra, Jr. Irrevocable Tr. v. Signature Bank Corp.*, 816 F. Supp. 2d 222, 236 (S.D.N.Y. 2011), *aff’d* 503 F. App’x 51 (2d Cir. 2012) (“As a preliminary matter, the breach of contract . . . claim[is] preempted by the New York U.C.C. Article 4-A . . . preclude[s] common law claims that would impose liability inconsistent with the rights and liabilities expressly created by [the article].”); *see also Golden Door V&I, Inc. v. TD Bank*, 999 N.Y.S.2d 510, 513 (N.Y. App. Div. 2d Dep’t 2014) (affirming dismissal of common law claims, including breach of contract, as precluded by Article 4-A); *I. Cruise.com Corp. v. Aliksanyan*, 847 N.Y.S.2d 896, 896 (N.Y. Sup. Ct. N.Y. Cty. 2007) (dismissing breach

of contract and negligence claims against defendant bank involving allegedly unauthorized wire transfers, as case law and legislative history showed that “[A]rticle 4-A of the UCC has preempted the field and exclusively governs electronic fund transfers”).

Imposing common law liability for the conduct about which BDA complains would be squarely inconsistent with the provisions of Article 4-A. BDA’s theories of common law negligence and breach of contract are facially contradicted by multiple sections of Article 4-A, including those cited by BDA in the Complaint. Setting aside its conclusory allegations, the Complaint simply alleges that Wells Fargo inappropriately processed unauthorized payment orders which were sent pursuant to the security procedures in the Agreement. Compl. ¶ 29. The Second Circuit recently examined precisely this issue, holding that the longer common law statute of limitations periods applicable to negligence and breach of contract claims alleging that the defendant bank wrongfully processed the wire transfers at issue were precluded by Article 4-A’s one-year statute of repose. *Ma*, 597 F.3d at 86-87, 90. Specifically, the Court noted that “Article 4A controls how electronic funds transfers are conducted and specifies certain rights and duties related to the execution of such transactions,” including the adoption of security procedures. *Id.* at 89. As a result, Article 4-A’s “provisions protect[ed] against the type of underlying injury or misconduct” alleged, and because all of the claims at issue were, “at their core, assertions that [plaintiff] did not order or approve any of the disputed electronic transfers of funds from his accounts, [it was] bound to recognize the rights and duties New York law provides for precisely these circumstances.” *Id.* at 89-90; *see also Signature Bank Corp.*, 816 F. Supp. 2d at 236 (breach of contract claim precluded because “[a]ny common law claims about the existence of unauthorized wire transfers . . . and the mechanics of how those transactions were conducted, fall[s] within the regime of Article[] 4-A”).

Allegations that Wells Fargo did not take reasonable steps to detect whether the payment orders at issue were fraudulent, or to confirm whether BDA authorized the wire transfers, are governed by Sections 4-A-202, 4-A-203, and 4-A-204 of the N.Y. U.C.C., which delineate when liability for fraudulent wire transfers is borne by the bank that received the payment order, or when the risk remains with sender or originator of the transfer instructions. *See generally* N.Y. U.C.C. §§ 4-A-202-204. Moreover, subject to certain inapplicable exceptions, the “rights and obligations arising under [Section 4-A-202] or Section 4-A-203 may not be varied by Agreement.”⁷ N.Y. U.C.C. § 4-A-202(6). As a result, any claim that Wells Fargo was obligated – either under a negligence theory or a misguided interpretation of the Agreement (Compl. ¶¶ 44, 72) – to investigate and determine the fraudulent source of the Unauthorized Transfers, which originated with BDA and contained its unique SWIFT BIC identifier (Compl. ¶¶ 20, 31; Compl. Ex. B; Ex. 3), is plainly inconsistent with the statutory framework of the N.Y. U.C.C. and would impose liability on receiving banks even when payment orders are “authorized” or “effective as the order of the customer.” N.Y. U.C.C. § 4-A-202(1)-(2); *see also Centre-Point Merch. Bank Ltd. v. Am. Express Bank Ltd.*, 913 F. Supp. 202, 208 (S.D.N.Y. 1996) (common law claims alleging that fraudulent payment orders were made “in breach of a duty to provide commercially reasonable security [and] dealing with security procedures and verification of payment orders” were precluded because of the “specific Article 4-A provisions concerning” such transactions,

⁷ In *Fischer & Mandell LLP v. Citibank*, the Second Circuit held that while plaintiff’s common law negligence claim was precluded by Article 4-A, 632 F.3d at 801, its breach of contract claim was not precluded under Article 4 of the N.Y. U.C.C. because it was not inconsistent with the rights and liabilities of Article 4 and because the parties were permitted to vary their respective rights and liabilities by agreement. *Id.* at 797-98. This is distinct from the facts at issue because (i) BDA’s claims here are governed by Article 4-A of the N.Y. U.C.C., (ii) Wells Fargo and BDA were not permitted to vary the rights and obligations at issue by agreement, N.Y. U.C.C. § 4-A-202(6), and (iii) BDA’s breach of contract claim is inconsistent with the terms of Article 4-A.

including Sections 4-A-202 and 4-A-204). Because BDA fails to state a claim under the N.Y. U.C.C., *see supra* Section I, the entirety of the Complaint, including BDA's common law claims, should be dismissed with prejudice. *See Fischer & Mandell LLP*, 632 F.3d at 801-02; *Golden Door*, 999 N.Y.S.2d at 513.

III. BDA Has Failed to State a Claim for Negligence in Any Event.

Assuming for the sake of argument that BDA's negligence claim is not precluded by Article 4-A of the N.Y. U.C.C., it has still failed to sufficiently allege a cause of action against Wells Fargo. In support of its negligence claim, BDA essentially offers one allegation – that Wells Fargo owed it a duty of care independent of the Agreement to implement and execute “know your customer” and other unspecified fraud detection policies, which Wells Fargo violated by failing to report and block the “anomalous” Unauthorized Transfers. Compl. ¶¶ 68-76. BDA argues that following this “simple reporting process would have revealed the scheme by outsiders and averted the losses resulting from the Unauthorized Transfers.” *Id.* ¶ 75. This argument fails.

A. The Agreement Prohibits Any Claim for Negligence.

As an initial matter, the Agreement governing the Relationship between Wells Fargo and BDA prohibits BDA's negligence claim. The Agreement states that “Wells Fargo's liability, if any, will be *limited* to those actual damages which are the direct result of Wells Fargo's *gross negligence* or *willful misconduct*.” Compl. Ex. A. ¶ 7.15 (emphasis added). In New York, “contractual provisions absolving a party from its own negligence are generally enforceable.” *Plaintiffs' State & Secs. Law Settlement Class Counsel v. Bank of N.Y. Mellon*, 985 N.Y.S.2d 398, 404 (N.Y. Sup. Ct. N.Y. Cty. 2014); *see also Colnaghi, U.S.A.*, 595 N.Y.S.2d at 381 (same).

BDA has not alleged that Wells Fargo was grossly negligent, and any subsequent amendment to the Complaint to add a claim for gross negligence would be futile given its current allegations. Gross negligence “differs in kind, not only degree, from claims of ordinary negligence” and is considered “conduct that evinces a reckless disregard for the rights of others or smacks of intentional wrongdoing.” *Colnaghi, U.S.A.*, 595 N.Y.S.2d at 381 (quotations omitted). In a “contract between sophisticated parties” such as BDA and Wells Fargo, “New York applies a more exacting standard of gross negligence than it would in other contexts.” *Alitalia Linee Aeree Italiane, S.P.A. v. Airline Tariff Publ’g Co.*, 580 F. Supp. 2d 285, 294 (S.D.N.Y. 2008). Under this standard, to avoid enforcement of a limited liability provision a plaintiff must show “reckless indifference or intentional wrongdoing.” *Id.*

For the same reason that it has failed to allege that Wells Fargo did not act in good faith under the N.Y. U.C.C., *see supra* Section I.A.2, BDA has not alleged that Wells Fargo was grossly negligent. As BDA admitted, the Unauthorized Transfers were sent from its internal computer system, from its own SWIFT terminal, were authenticated by SWIFT, and appeared identical to validly authorized payment orders. Compl. ¶¶ 18, 20, 31; Compl. Ex. B. Nowhere in the Complaint does BDA allege that Wells Fargo *knew* that the Unauthorized Transfers were the result of fraudulent payment orders and *intentionally* processed the orders despite knowing that they were unauthorized. Far from displaying “reckless indifference,” Wells Fargo ensured that the payment orders originated from BDA and were authenticated in accordance with the Agreement prior to initiating the transfers. Compl. ¶¶ 20, 31; Compl. Ex. B; Ex. 3; *see also supra* Section I.A. Allegations that Wells Fargo “should have” instituted policies that “should have” triggered a reporting process that might have then alerted BDA of the Unauthorized Transfers are a far cry from asserting that Wells Fargo knew of the underlying fraud. Compl.

¶¶ 70-74. BDA has therefore failed to allege gross negligence, and due to the Agreement's limitation of liability clause prohibiting BDA from bringing a claim of ordinary negligence, BDA's third cause of action should be dismissed with prejudice. *See Plaintiffs' State*, 985 N.Y.S.2d at 404-05 (dismissing claim for failure to allege gross negligence where contract at issue provided that defendant bank "shall not be liable for damages or claims . . . except . . . for its own bad faith, gross negligence or willful misconduct") (quotations omitted).

B. Wells Fargo Did Not Owe BDA a Duty of Care Independent of the Agreement.

New York law has long held that "[t]he legal relationship between a bank and its customer is a contractual one of debtor and creditor." *Elite Investigations*, 2006 WL 3232185, at *5; *see also Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Chemical Bank*, 456 N.Y.S.2d 742, 745 (N.Y. 1982) (same). Indeed, a bank has a duty only to its customers, as established by contractual relationship. *See, e.g., Lerner v. Fleet Bank, N.A.*, 459 F.3d 273, 286 (2d Cir. 2006) (acknowledging that "a bank has no duty to customers of other banks") (quotation omitted). Because the Relationship between BDA and Wells Fargo was governed by the Agreement, BDA is prohibited from bringing a negligence claim that arises out of the duties that Wells Fargo owed BDA under the contract. As noted by the Court of Appeals, it is a "well-established principle that a simple breach of contract is not to be considered a tort unless a legal duty independent of the contract has been violated." *Clark-Fitzpatrick, Inc. v. Long Island R.R. Co.*, 521 N.Y.S.2d 653, 656 (N.Y. 1987). In order to successfully maintain a tort claim against a defendant arising out of a contractual relationship, a plaintiff must demonstrate that the defendant owed a duty that "spring[s] from circumstances extraneous to, and not constituting elements of, the contract." *Id.* at 656-57. This prohibits customers from bringing negligence actions against their banks for claims that arise out of the bank-customer relationship. *See Centre-Point*, 913 F. Supp. at 208-

09 (dismissing a negligence claim because the duty that defendant bank allegedly breached was identical to plaintiff's concurrent breach of contract claim); *Calisch Assocs. Inc. v. Mfrs. Hanover Tr. Co.*, 542 N.Y.S.2d 644, 645-46 (N.Y. App. Div. 1st Dep't 1989).

The only duty at issue here – Wells Fargo's obligation to process authenticated payment orders sent from BDA – is governed by the Agreement, and Wells Fargo did not owe BDA any duties other than those that stemmed from the Agreement and which it allegedly violated. It is clear that BDA's negligence claim is nothing more than a transparent attempt to re-fashion its breach of contract claim. *Compare* Compl. ¶ 40 (alleging Wells Fargo breached the Agreement by failing to “follow ‘know your customer’ and fraud detection policies and procedures designed to detect and deter suspicious activity”) *with id.* ¶ 71 (alleging that Wells Fargo was negligent because it did not “implement and follow ‘know your customer’ and fraud detection policies and procedures designed to monitor for suspicious activity”). This is not permitted under New York law.⁸ *See Elite Investigations*, 2006 WL 3232185, at *4-5 (dismissing negligence claim involving fraudulent fund transfers because transfers were authorized under Article 4-A and defendant bank did not breach its customer agreement).

C. Wells Fargo Had No Duty to Prevent the Unauthorized Access of BDA's Internal Systems.

Even if one disregards the fact that BDA's negligence claim is both precluded by Article 4-A and prohibited by the Agreement, the “independent” duty of care that BDA purports to identify *still* does not give rise to liability against Wells Fargo. As recently held by the Eastern District, internal “know your customer” policies “cannot form the basis for a negligence claim.” *Silverman Partners*, 687 F. Supp. 2d at 282. The “know your customer” and anti-money

⁸ As stated in Section II, above, both BDA's negligence and breach of contract claims are in any event precluded by Article 4-A of the N.Y. U.C.C. Courts hold that Article 4-A precludes common law claims that are inconsistent with its terms precisely to avoid the kind of duplicative pleading that BDA hopes to accomplish with its Complaint.

laundering policies upon which BDA attempts to rely, *see, e.g.*, Compl. ¶ 14 n.1, were not created to protect customers such as BDA or to impose upon banks a duty to their customers. *See Silverman Partners*, 687 F. Supp. 2d at 282 (noting that the rules cited by plaintiff, including “know your customer” policies and the USA PATRIOT Act were “intended to protect the [defendant] banks and the general public from harm” and were “not created to protect borrowers”); *see also supra* Section I.C. And compliance with these laws and policies does not impose upon Wells Fargo an obligation to monitor BDA’s internal computer systems and guard against the theft of BDA employee log-in information.

Here, BDA has admitted that the fraudulent payment orders were caused by a breach of its own security via the theft of its employee information. Compl. ¶¶ 20, 23, 31; Ex. 4 at 2-3. New York courts have acknowledged that in similar circumstances, it is the plaintiff who is in the best position to guard against fraud, and therefore cannot shift liability to a defendant bank or payment processing company. *See Centre-Point*, 2000 WL 1772874, at *5-6 (dismissing Article 4-A claim and noting that “although Plaintiff alleges that Defendant’s failure to comply [with the agreed-upon security procedure] is implicit in its failure to identify the fraud . . . Plaintiff was in a much better position than Defendant to do so” because the fraud was effectuated by telexes altered in Plaintiff’s “telex room and telex machines”); *Getty Petroleum Corp. v. Am. Express Travel Related Servs. Co., Inc.*, 660 N.Y.S.2d 689, 692-93 (N.Y. 1997) (dismissing claims against defendant credit card company for honoring fraudulent checks, noting that plaintiff “was in the best position to prevent the losses” by keeping a more watchful eye on its employees and examining its records).

IV. Wells Fargo Did Not Breach the Agreement.

In order to allege a claim of breach of contract under New York law, a plaintiff must show (i) a contract; (ii) adequate performance by one party; (iii) breach by the other party; and

(iv) damages. *First Inv'rs Corp. v. Liberty Mut. Ins. Co.*, 152 F.3d 162, 168 (2d Cir. 1998). In demonstrating a breach, a plaintiff must allege with specificity the contractual provision that it claims was breached. *See Kraus v. Visa Int'l Serv. Ass'n*, 756 N.Y.S.2d 853, 853 (N.Y. App. Div. 1st Dep't 2003). In support of its claim, BDA inappropriately attempts to incorporate into the Agreement's general language about compliance with applicable laws and banking practices unspecified "know your customer" and fraud detection policies that are not contained in the contract and which it claims Wells Fargo breached by "failing to detect, block and report the Unauthorized Transfers." Compl. ¶¶ 40-44.

The Agreement governing the Relationship between Wells Fargo and BDA stated that Wells Fargo's only responsibility with respect to the payment orders at issue was to verify that they were properly authenticated by SWIFT in accordance with the agreed-upon security procedure. Compl. Ex. A ¶ 3.1. BDA further agreed that it would "utilize authenticated SWIFT message formats" and that "Wells Fargo will be entitled to rely upon all such messages *appearing* to have been sent by [BDA]." *Id.* ¶ 2.1 (emphasis added). The Agreement says nothing about the "know your customer" guidelines or fraud detection policies that BDA attempts to incorporate. Nor does BDA point to any proof that such unnamed and unspecified policies are included in "general banking practices" aside from the conclusory allegation that they are implemented by anonymous "commercial banks in the United States." Compl. ¶ 40. The only evidence that BDA appears to have been able to marshal in support of its claim is the wholly unsupported allegation that Wells Fargo "boasted" to BDA of a program which might have alerted it to the Unauthorized Transfers. *Id.* ¶¶ 14, 41-43. However, this alleged "boast" is not part of BDA's Agreement with Wells Fargo.

When entering into the Relationship, BDA acknowledged that the Agreement constituted

the “entire agreement and understanding” between the parties and that it “may not be changed orally.” Compl. Ex. A. ¶ 7.19. New York courts have consistently held that this type of merger clause expressly forbids reliance on any representation not specifically contained in the contract at issue. *See Brower v. Nydic, Inc.*, 1 F. Supp. 2d 325, 327 (S.D.N.Y. 1998) (dismissing a claim based on an oral representation because the relevant contract stated that the written agreement “contain[ed] the entire understanding of the parties”) (quotation omitted); *Xi Mei Jai*, 981 N.Y.S.2d at 80-81 (holding that a contract’s merger clause “foreclose[d plaintiff’s] reliance upon any representation not contained in the . . . agreement”). Indeed, New York expressly mandates that when a written contract contains a clause stating that it cannot be changed orally, such as the Agreement at issue, any modification must also be made in writing. N.Y. GEN. OBLIG. § 15-301(1); *see also SAA-A, Inc. v. Morgan Stanley Dean Witter & Co.*, 721 N.Y.S.2d 640, 642 (N.Y. App. Div. 1st Dep’t 2001) (noting that Section 15-301 prohibits oral modification of a contract that requires any amendment be in writing). As a result, any representation that Wells Fargo might have made to BDA concerning fraud detection policies that is not contained in the Agreement is simply irrelevant to an analysis of whether Wells Fargo breached the Agreement.

Moreover, *even if* any alleged representation made by Wells Fargo regarding fraud detection policies could be incorporated into the Agreement, the Complaint proves that BDA simply misinterprets such policies. BDA alleges that Wells Fargo represented that its fraud detection policies were “designed to comply with the various laws of the United States,” specifically the Bank Secrecy Act and those regarding money laundering. Compl. ¶¶ 14, 14 n.1. It is these transactions – those potentially involving money laundering or terrorism – that Wells Fargo allegedly represented would be monitored for, screened, and reported. As explained above, *see supra* Sections I.C and III.C, and as noted in the Agreement, Wells Fargo’s

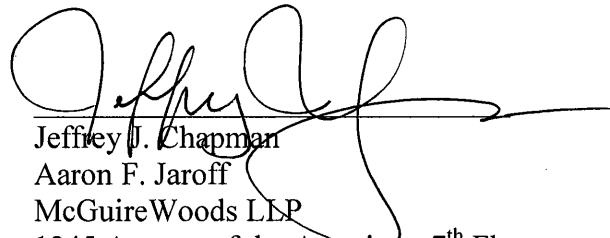
compliance with these regulations was not intended to protect customers against the hacking of their internal computer systems, but rather to ensure that Wells Fargo obeyed rules set by OFAC and did not inadvertently finance international terrorism. Compl. Ex. A ¶ 7.8. BDA attempts to impose these additional obligations on Wells Fargo because it knows that it cannot show that Wells Fargo failed to perform exactly as the parties contemplated under the actual terms of the Agreement. *See Elite Investigations*, 2006 WL 3232185, at *4-5 (holding that defendant bank did not breach its agreement because the fund transfer orders at issue appeared to be validly authorized and, as a result, the bank “had no practical way to determine” that the payment orders were fraudulent).

CONCLUSION

For the foregoing reasons, Wells Fargo respectfully requests that the Complaint be dismissed in its entirety, with prejudice.

Dated: New York, New York
February 18, 2016

By:



Jeffrey J. Chapman
Aaron F. Jaroff
McGuireWoods LLP
1345 Avenue of the Americas, 7th Floor
New York, New York 10105-0106
(212) 548-2100
jchapman@mcguirewoods.com
ajaroff@mcguirewoods.com

Attorneys for Defendant Wells Fargo Bank, N.A.